LẬP TRÌNH MẠNG CĂN BẢN

Biên soạn: ThS. Đỗ Thị Hương Lan

TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG
FACULTY OF COMPUTER NETWORK AND COMMUNICATIONS
Tầng 8 - Tòa nhà E, trường ĐH Công nghệ Thông tin, ĐHQG-HCM

Chương 11

Bảo mật – Mã hóa

Nội dung chi tiết

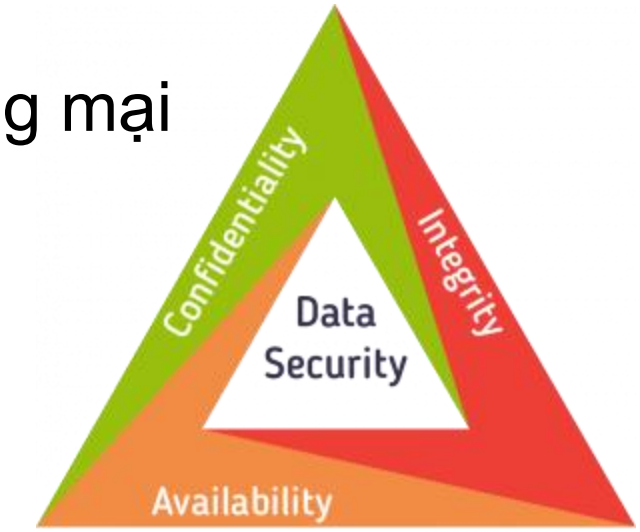
- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

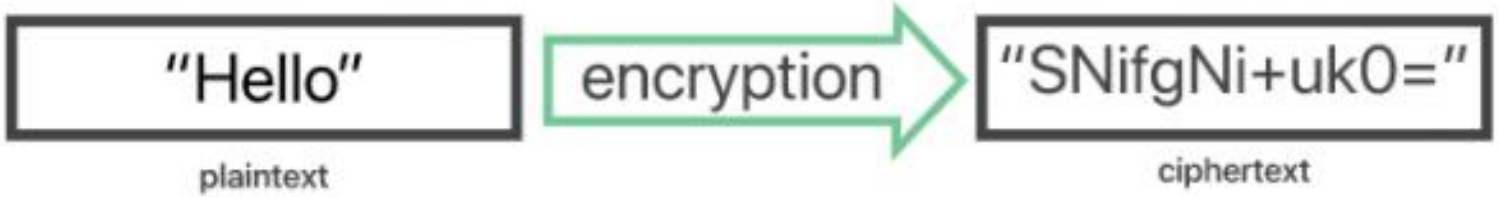
Nội dung chi tiết

- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

Giới thiệu

- **Bảo mật**
  - Vấn đề hết sức quan trọng trong giao dịch thương mại và nhiều kiểu trao đổi thông tin khác
    - **Tính mật** của thông tin **(Confidentiality)**
    - **Tính toàn vẹn** thông tin **(Integrity)**
    - **Tính sẵn sàng** của hệ thống **(Availability)**
- **Mã hóa**
  - **Plaintext → Cipher text**





Giới thiệu

Results | Messages

	USERNAME	PASSWORD	HOTEN	DIENTHOAI	CHUCVU	MAKHOA
1	admin	21232F297A57A5A743894AE4A801FC3	Trần	NULL	NULL	0
2	admin1	E0CF25AD42683B3DF678C61F42C6BDA	NULL	NULL	NULL	0
3	CNPM	747FC2989F7EADC7ED4F490BC9FC65A	NULL	NULL	NULL	CNPM
4	HTTT	8823247E8CA93837D44ABD6548B74ECA	NULL	NULL	NULL	HTTT
5	KHMT	39CB116725EA22A3AB6824DF7954E29	NULL	NULL	NULL	KHMT
6	KTMT	76789B92E773FB61FD67715B048769D	NULL	NULL	NULL	KTMT
7	MMT	3272CA43DFEC08F03EB95CE1D2F4D9	NULL	NULL	NULL	MMT

Query executed successfully. | VP\SQL2008 (10.0 RTM)

Minh họa về Mã hóa (Password)

Giới thiệu

- Có rất nhiều loại phương pháp mã hóa khác nhau với ưu và nhược điểm riêng.
- **Phương pháp mã hóa**:
  - Mã hóa cổ điển
  - Mã hóa một chiều
  - Mã hóa đối xứng
  - Mã hóa bất đối xứng

Các thuật ngữ

- **Plain text** (bản rõ): dữ liệu chưa mã hóa
- **Cipher text** (bản mã): dữ liệu đã được mã hóa
- **Key**: dữ liệu dùng để mã hóa hoặc giải mã
- **Cryptographic algorithm hoặc Cipher**: giải thuật mã hóa hoặc giải mã
- **Strength**: độ khó khi bẻ khóa

Phá mã

- **Phá mã**
  - Giải mã văn bản đã được mã hóa không biết trước khóa bí mật

- **Phương pháp phá mã**
  - **Vét cạn**
    - Thử tất cả các khóa có thể
  - **Thám mã**
    - Khai thác những nhược điểm của giải thuật
    - Dựa trên những đặc trưng chung của nguyên bản hoặc một số cặp nguyên bản - bản mã mẫu

Phá mã

- **Phá mã**
  - Giải mã văn bản đã được mã hóa không biết trước khóa bí mật

- **Phương pháp phá mã**
  - **Vét cạn**
    - Thử tất cả các khóa có thể
  - **Thám mã**
    - Khai thác những nhược điểm của giải thuật
    - Dựa trên những đặc trưng chung của nguyên bản hoặc một số cặp nguyên bản - bản mã mẫu

Phương pháp phá mã vét cạn

- Về lý thuyết có thể thử tất cả các giá trị khóa cho đến khi tìm thấy nguyên bản từ bản mã
- Dựa trên giả thiết có thể nhận biết được nguyên bản cần tìm
- Thực tế không khả khi nếu độ dài khóa lớn

Thời gian tìm kiếm trung bình

Kích thước khóa (bit)	Số lượng khóa	Thời gian cần thiết (1 giải mã/μs)	Thời gian cần thiết (10^6 giải mã/μs)
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 phút	2,15 ms
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1142 năm	10,01 giờ
128	$2^{128} = 3{,}4 \times 10^{38}$	2^{127} μs = $5{,}4 \times 10^{24}$ năm	$5{,}4 \times 10^{18}$ năm
168	$2^{168} = 3{,}7 \times 10^{50}$	2^{167} μs = $5{,}9 \times 10^{36}$ năm	$5{,}9 \times 10^{30}$ năm
26 ký tự (hoán vị)	$26! = 4 \times 10^{26}$	2×10^{26} μs = $6{,}4 \times 10^{12}$ năm	$6{,}4 \times 10^6$ năm

Khóa DES dài 56 bit
Khóa AES dài 128+ bit
Khóa 3DES dài 168 bit

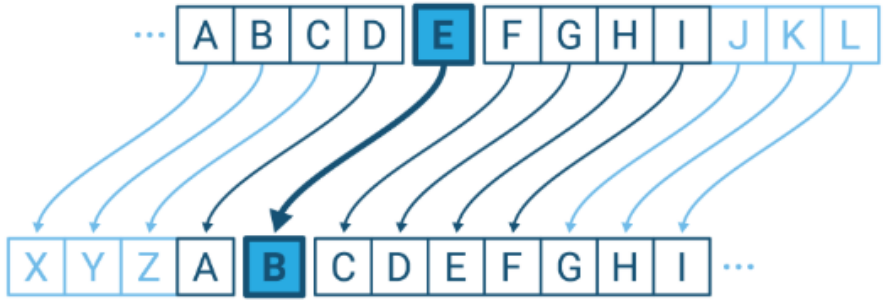
Tuổi vũ trụ: ~ 10^{10} năm

Nội dung chi tiết

- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

Mã hóa cổ điển

- **Mã hóa cổ điển**
  - Mã hóa hoán vị và mã hóa thay thế
  - Mã hóa Caesar
  - Mã hóa Vigenère
  - Mã hóa Playfair



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

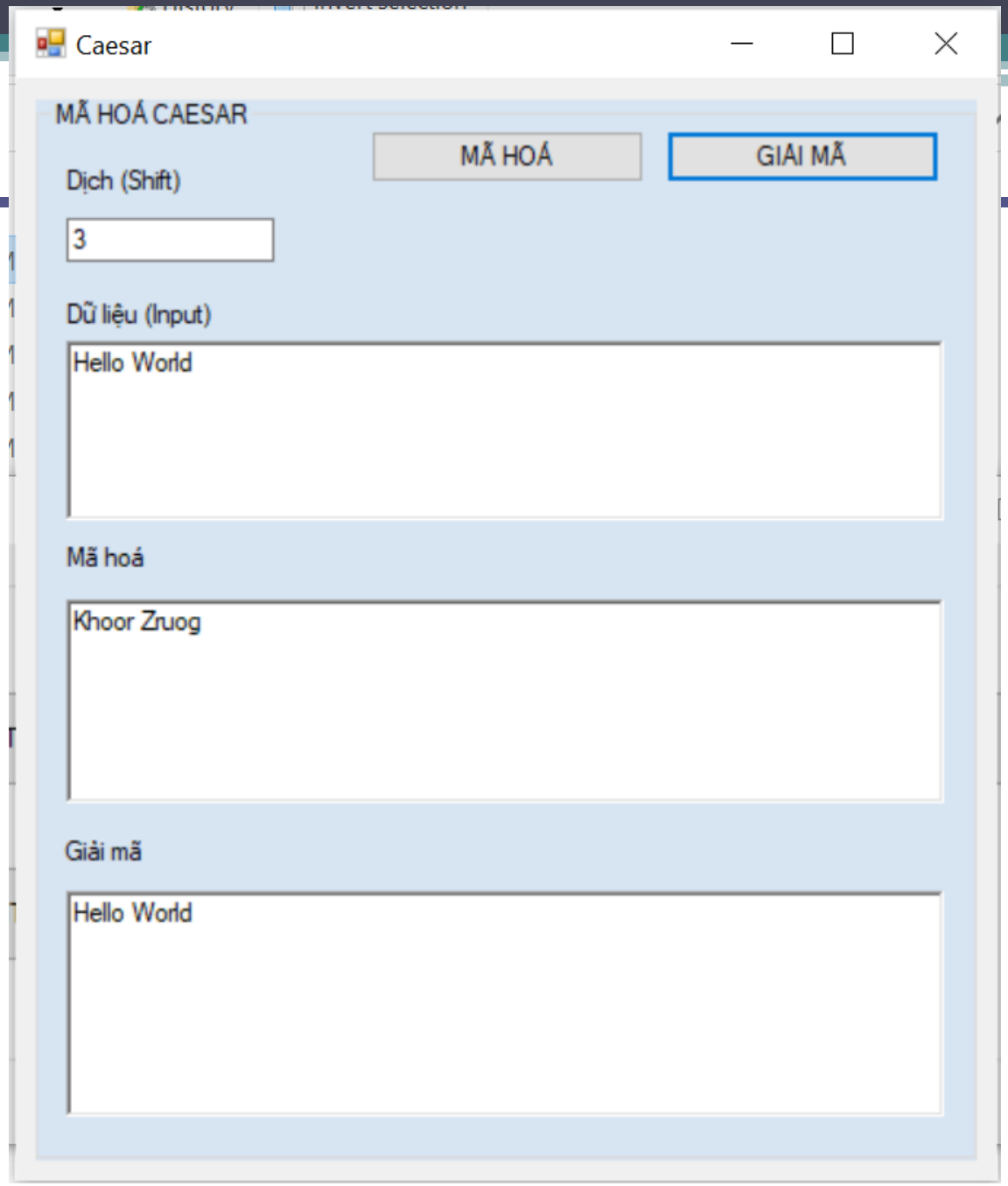
Ví dụ

- Phá mã **Caesar**
  - Bản mã: GCUA VQ DTGCM
  - Bản mã: Mfyj Htani Anwzx

- Phá mã **Vigenère**
  - Bản mã: iyhiehbgaawac
  - Key: antn

Ví dụ

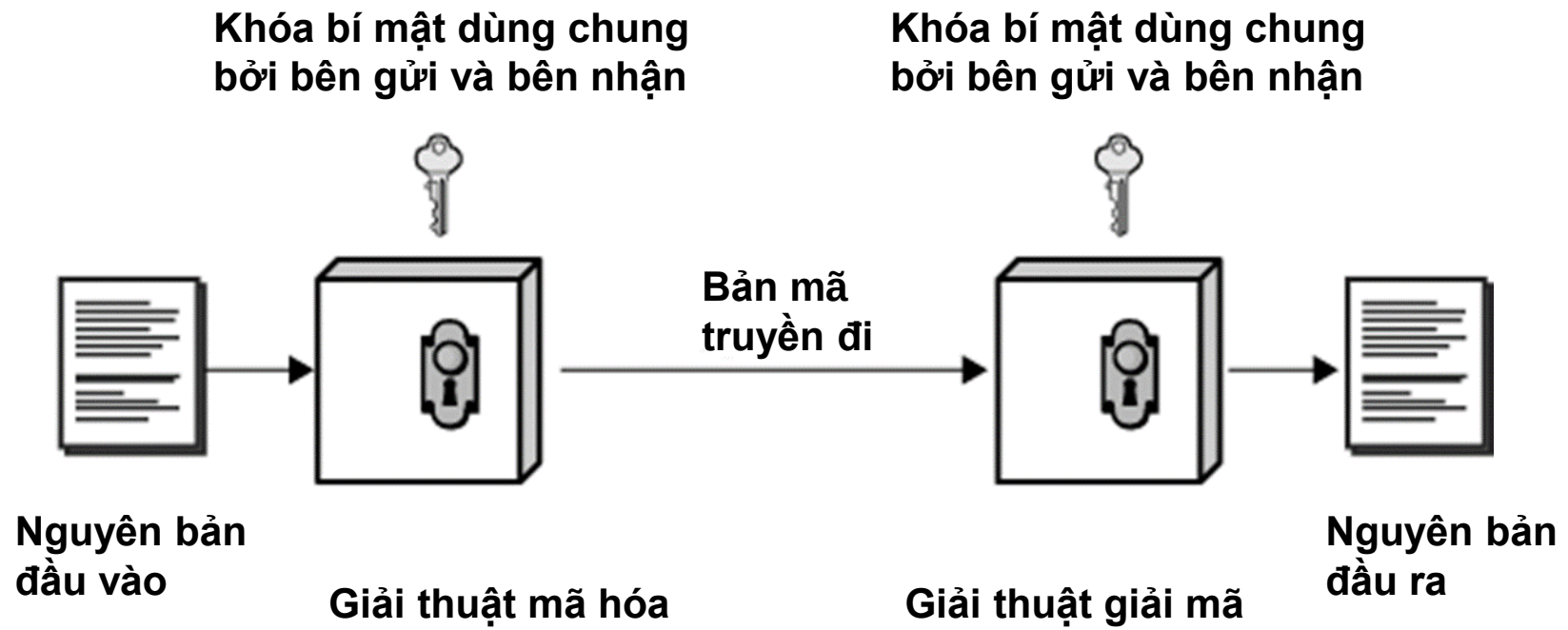
- Mã hóa **Caesar**
  - P: **Hello World**
  - Shift: 3
  - C: **Khoor Zroug**



Nội dung chi tiết

- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

Mã hóa đối xứng



Mã hóa

$Y = E_K(X)$

Giải mã

$X = D_K(Y)$

Mô hình Mã hóa đối xứng

- Gồm có 5 thành phần
  - Bản rõ
  - Giải thuật mã hóa
  - Khóa bí mật
  - Bản mã
  - Giải thuật giải mã
- **Độ an toàn**
  - Phụ thuộc vào **bí mật của khóa**, không phụ thuộc vào bí mật của giải thuật

DES (Data Encryption Standard)

- DES (Data Encryption Standard) được công nhận chuẩn năm 1977
- Tên giải thuật là DEA (Data Encryption Algorithm)
- Kích thước khối: 64 bit
- Kích thước khóa: 56 bit
- Số vòng: 16
- Từng gây nhiều tranh cãi về độ an toàn

Phá mã DES

- Khóa 56 bit có $2^{56} = 7,2 \times 10^{16}$ giá trị có thể
- Tốc độ tính toán cao có thể phá được khóa
  - 1997: 70000 máy tính phá mã DES trong 96 ngày
  - 1998: Electronic Frontier Foundation (EFF) phá mã DES bằng máy chuyên dụng (250000$) trong < 3 ngày
  - 1999: 100000 máy tính phá mã trong 22 giờ
- Vấn đề còn phải nhận biết được nguyên bản
- Nếu cần an toàn hơn: 3DES hay chuẩn mới AES

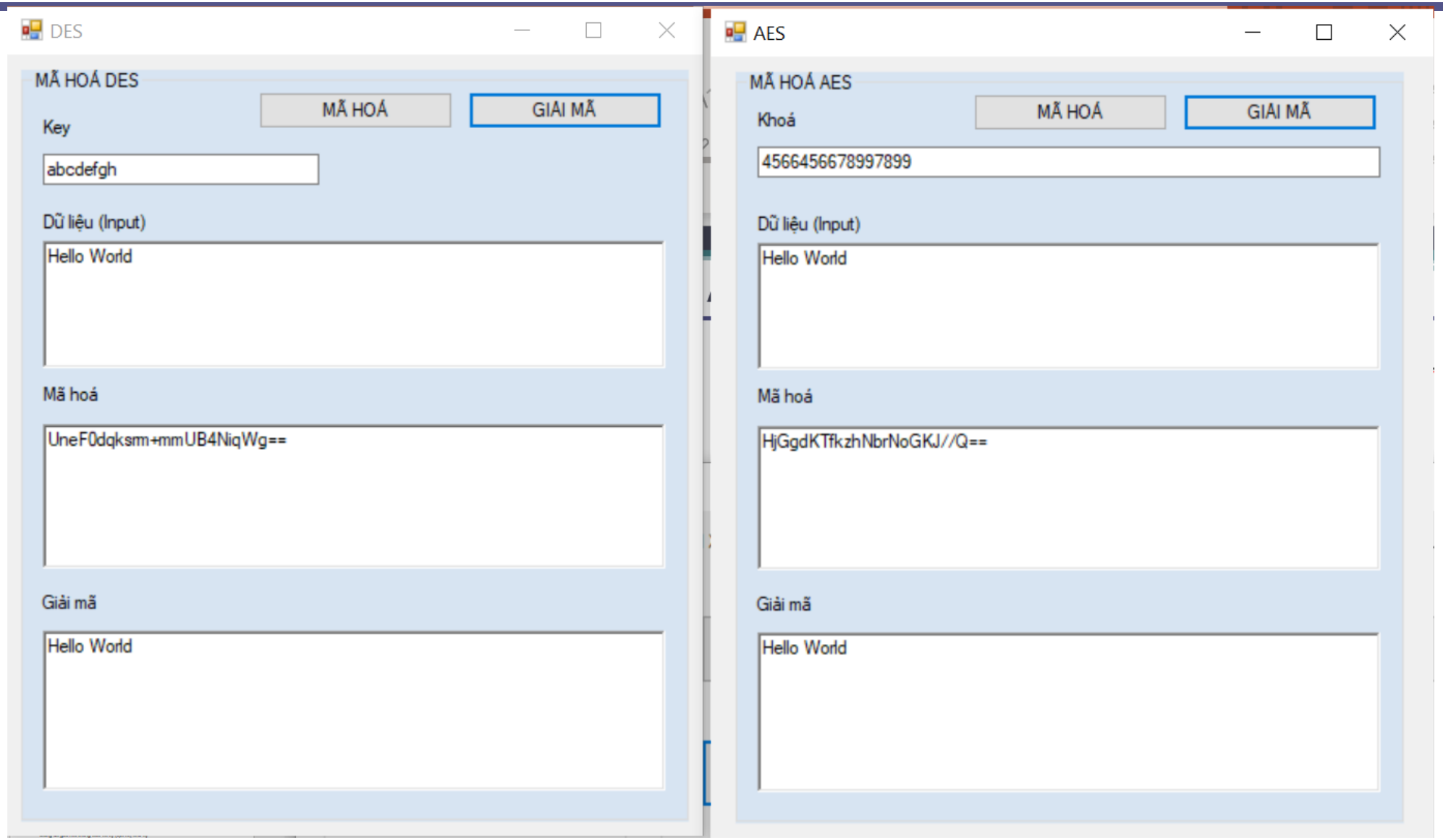
Hệ mã hóa 3DES

- Sử dụng 3 khóa và chạy 3 lần giải thuật DES
  - Mã hóa: $C = E_{K_3}[D_{K_2}[E_{K_1}[p]]]$
  - Giải mã: $p = D_{K_1}[E_{K_2}[D_{K_3}[C]]]$
- Độ dài khóa thực tế là 168 bit
  - Không tồn tại $K_4 = 56$ sao cho $C = E_{K_4}(p)$
- Vì sao 3 lần? tránh tấn công "gặp nhau ở giữa"
  - $C = E_{K_2}(E_{K_1}(p)) \Rightarrow X = E_{K_1}(p) = D_{K_2}(C)$
  - Nếu biết một cặp (p, C)
    - Mã hóa p với 2^{56} khóa và giải mã C với 2^{56} khóa
    - So sánh tìm ra K_1 và K_2 tương ứng
    - Kiểm tra lại với 1 cặp (p, C) mới; nếu OK thì K_1 và K_2 là khóa

AES - Chuẩn mã hóa tiên tiến

- AES (Advanced Encryption Standard) được công nhận chuẩn mới năm 2001
- Tên giải thuật là Rijndael (Rijmen + Daemen)
- An toàn hơn và nhanh hơn 3DES
- Kích thước khối: 128 bit
- Kích thước khóa: 128/192/256 bit
- Số vòng: 10/12/14

Ví dụ: DES và AES



Nội dung chi tiết

- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

Mã hóa bất đối xứng

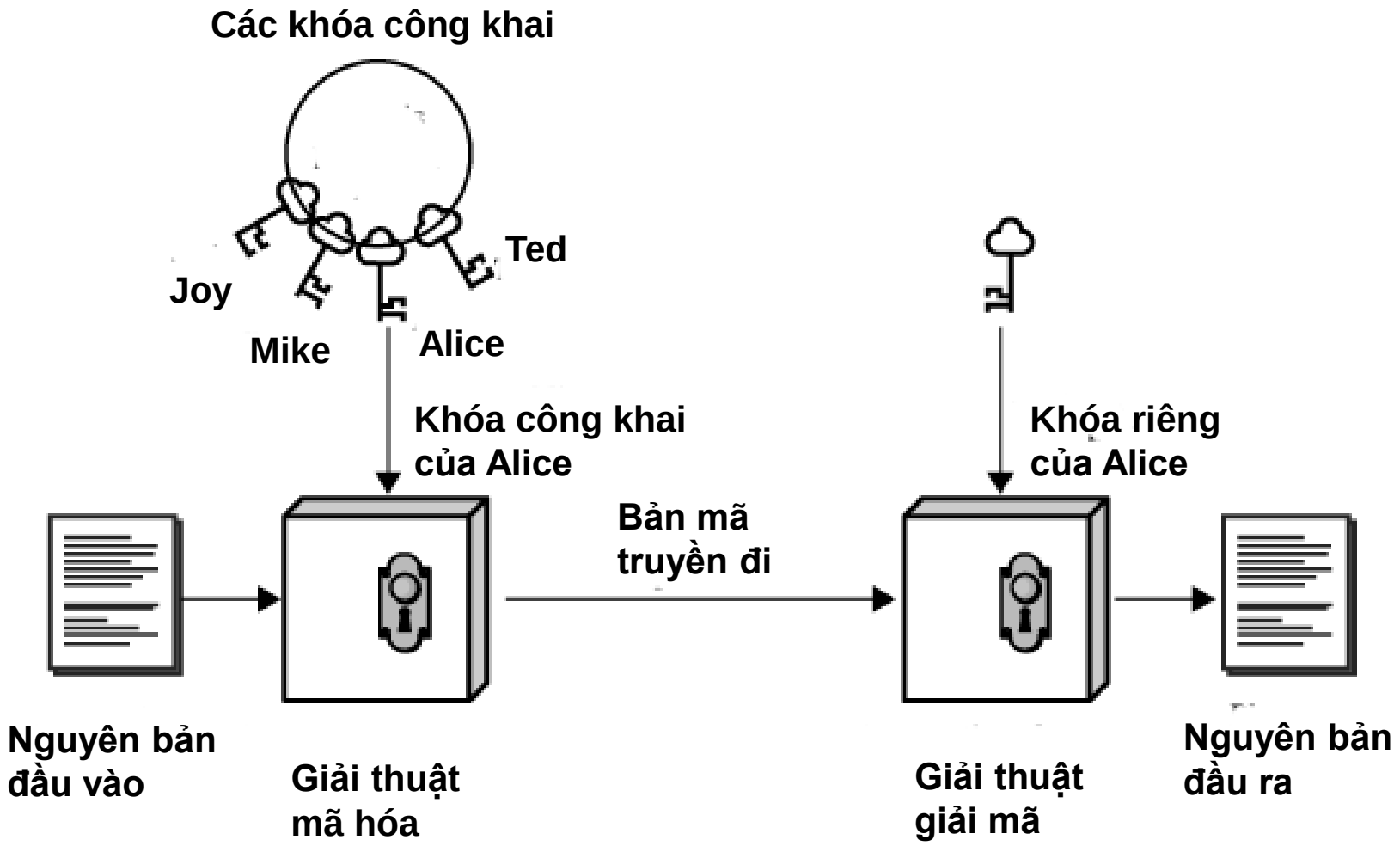
- Những hạn chế của mật mã đối xứng
  - Vấn đề phân phối khóa
    - Khó đảm bảo chia sẻ mà không làm lộ khóa bí mật
    - Trung tâm phân phối khóa có thể bị tấn công
  - Không thích hợp cho chữ ký số
    - Bên nhận có thể làm giả thông báo nói nhận được từ bên gửi

- Mật mã khóa công khai đề xuất bởi Whitfield Diffie và Martin Hellman vào năm 1976
  - Khắc phục những hạn chế của mật mã đối xứng
  - Có thể coi là bước đột phá quan trọng nhất trong lịch sử của ngành mật mã
  - Bổ sung chứ không thay thế mật mã đối xứng

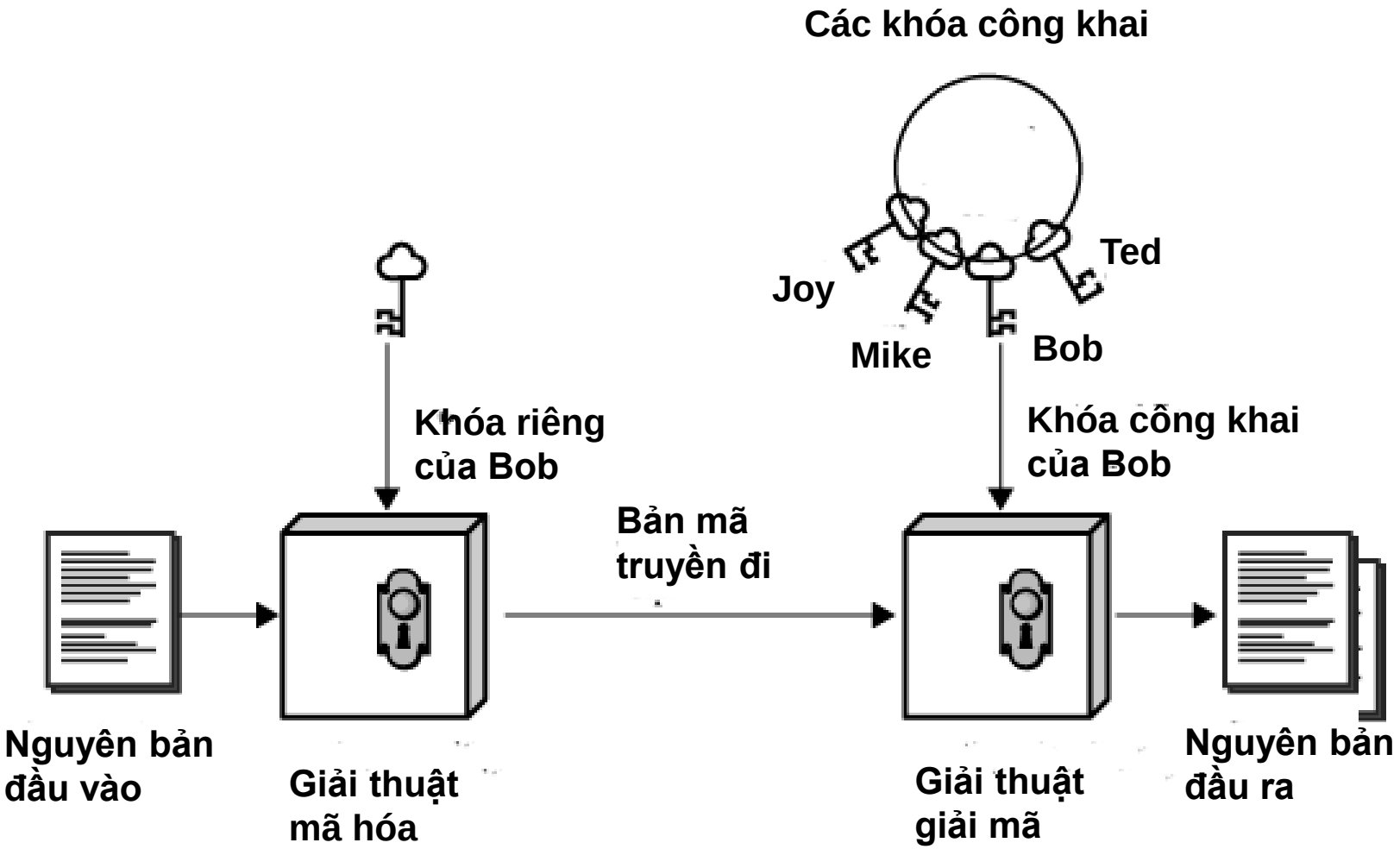
Đặc điểm mã hóa khóa công khai

- Còn gọi là mật mã hai khóa hay bất đối xứng
- Các giải thuật khóa công khai sử dụng 2 khóa
  - Một khóa công khai
    - Ai cũng có thể biết
    - Dùng để mã hóa thông báo và thẩm tra chữ ký
  - Một khóa riêng
    - Chỉ nơi giữ được biết
    - Dùng để giải mã thông báo và ký (tạo ra) chữ ký
- Có tính bất đối xứng
  - Bên mã hóa không thể giải mã thông báo
  - Bên thẩm tra không thể tạo chữ ký

Mã hóa khóa công khai



Xác thực


Các khóa công khai
Joy
Ted
Mike
Bob
Khóa riêng
của Bob
Khóa công khai
của Bob
Bản mã
truyền đi
Nguyên bản
đầu vào
Giải thuật
mã hóa
Giải thuật
giải mã
Nguyên bản
đầu ra

Ứng dụng mã hóa khóa công khai

- Có thể phân ra 3 loại ứng dụng
  - Mã hóa/giải mã

    Đảm bảo sự bí mật của thông tin
  - Chữ ký số

    Hỗ trợ xác thực văn bản
  - Trao đổi khóa

    Cho phép chia sẻ khóa phiên trong mã hóa đối xứng
- Một số giải thuật khóa công khai thích hợp cho cả 3 loại ứng dụng; một số khác chỉ có thể dùng cho 1 hay 2 loại

Hệ mã hóa RSA

- Đề xuất bởi Ron Rivest, Adi Shamir và Len Adleman (MIT) vào năm 1977
- Hệ mã hóa khóa công khai thông dụng nhất
- Mã hóa khối với mỗi khối là một số nguyên < n

  Thường kích cỡ n là 1024 bit ≈ 309 chữ số thập phân
- An toàn vì chi phí phân tích thừa số của một số nguyên lớn là rất lớn

Sự hỗ trợ giữ 2 hệ thống mã hóa

Giao thức bảo mật sử dụng cả 2:

- Đối xứng: bảo vệ trao đổi dữ liệu qua mạng, tốc độ xử lý nhanh
- Bất đối xứng: thành lập kết nỗi gữa 2 thực thể mạng và thành lập khóa đối xứng.

An ninh của RSA

- Khóa 128 bit là một số giữa 1 và một số rất lớn

  340.282.366.920.938.000.000.000.000.000.000.000.000

- Có bao nhiêu số nguyên tố giữa 1 và số này

  $\approx n / \ln(n) = 2^{128} / \ln(2^{128}) \approx$

  3.835.341.275.459.350.000.000.000.000.000.000.000

- Cần bao nhiêu thời gian nếu mỗi giây có thể tính được 10^{12} số

  Hơn 121.617.874.031.562.000 năm (khoảng 10 triệu lần tuổi của vũ trụ)

Phá mã RSA

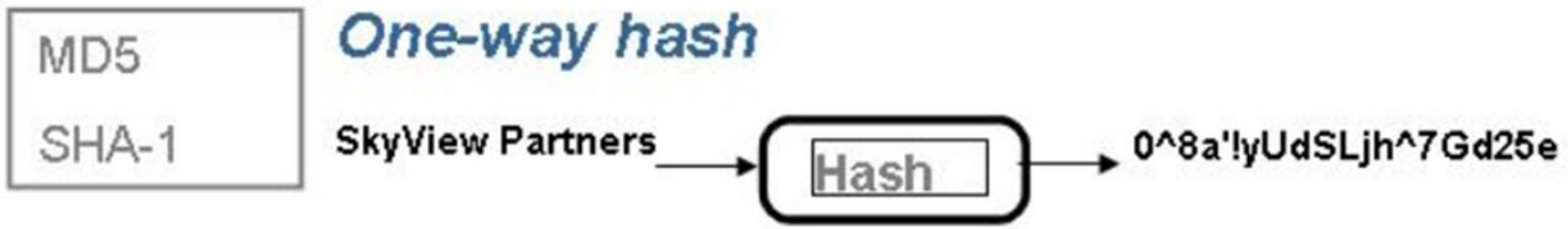
- Phương pháp vét cạn
  - Thử tất cả các khóa riêng có thể
    - Phụ thuộc vào độ dài khóa
- Phương pháp phân tích toán học
  - Phân n thành tích 2 số nguyên tố p và q
  - Xác định trực tiếp $\Phi(n)$ không thông qua p và q
  - Xác định trực tiếp d không thông qua $\Phi(n)$
- Phương pháp phân tích thời gian
  - Dựa trên việc đo thời gian giải mã
  - Có thể ngăn ngừa bằng cách làm nhiễu

Nội dung chi tiết

- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

Hash functions

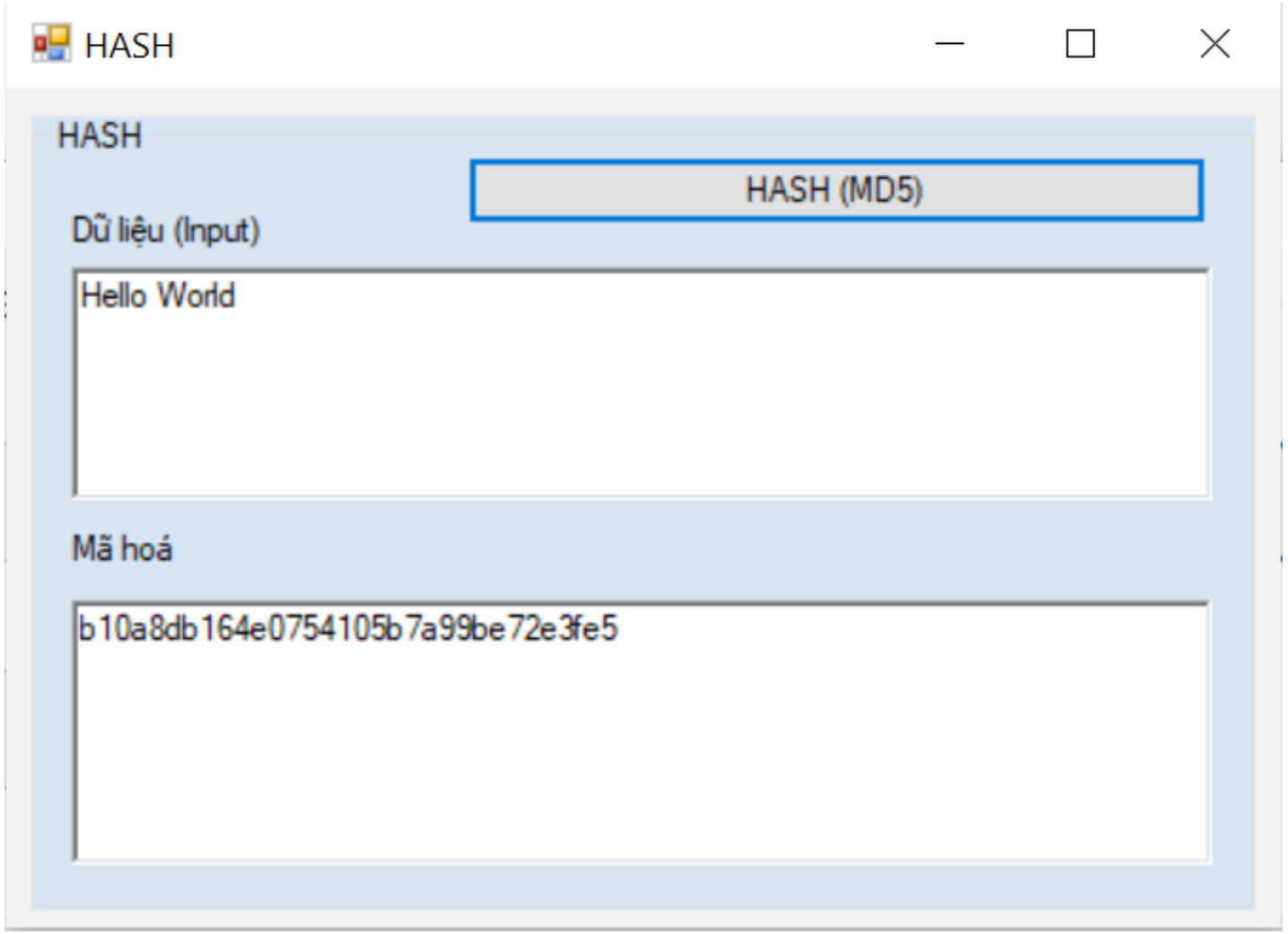
- Băm từng chuỗi bit một
- Không thể khôi phục dữ liệu ban đầu từ cipher text
- 1 bit khác nhau sẽ tạo ra ít nhất nữa số bit kết quả khác nhau



Hash functions

- MD (Message Digest) functions
  MD2, MD4, MD5: 16 bytes fingerprint
- SHA-1 (Secure Hash Algorithm-1): 20 bytes
- SHA-256: 256 bytes
- SHA-224: 224 bytes
- SHA-512: 512 bytes

Ví dụ: MD5


HASH
HASH
HASH (MD5)
Dữ liệu (Input)
Hello World
Mã hoá
b10a8db164e0754105b7a99be72e3fe5

Nội dung chi tiết

- Giới thiệu
- Mã hóa cổ điển
- Mã hóa đối xứng
- Mã hóa bất đối xứng
- Mã hóa một chiều (băm)
- Chữ ký điện tử

Chữ ký điện tử

- MAC (Message Authentication Code), chữ ký điện tử có hai mục tiêu:
  - Kiểm tra tính nguyên thủy (nguồn gốc)
  - Kiểm tra toàn vẹn của dữ liệu
- Sử dụng hash functions, symmetric hoặc asymmetric keys

Chữ ký điện tử

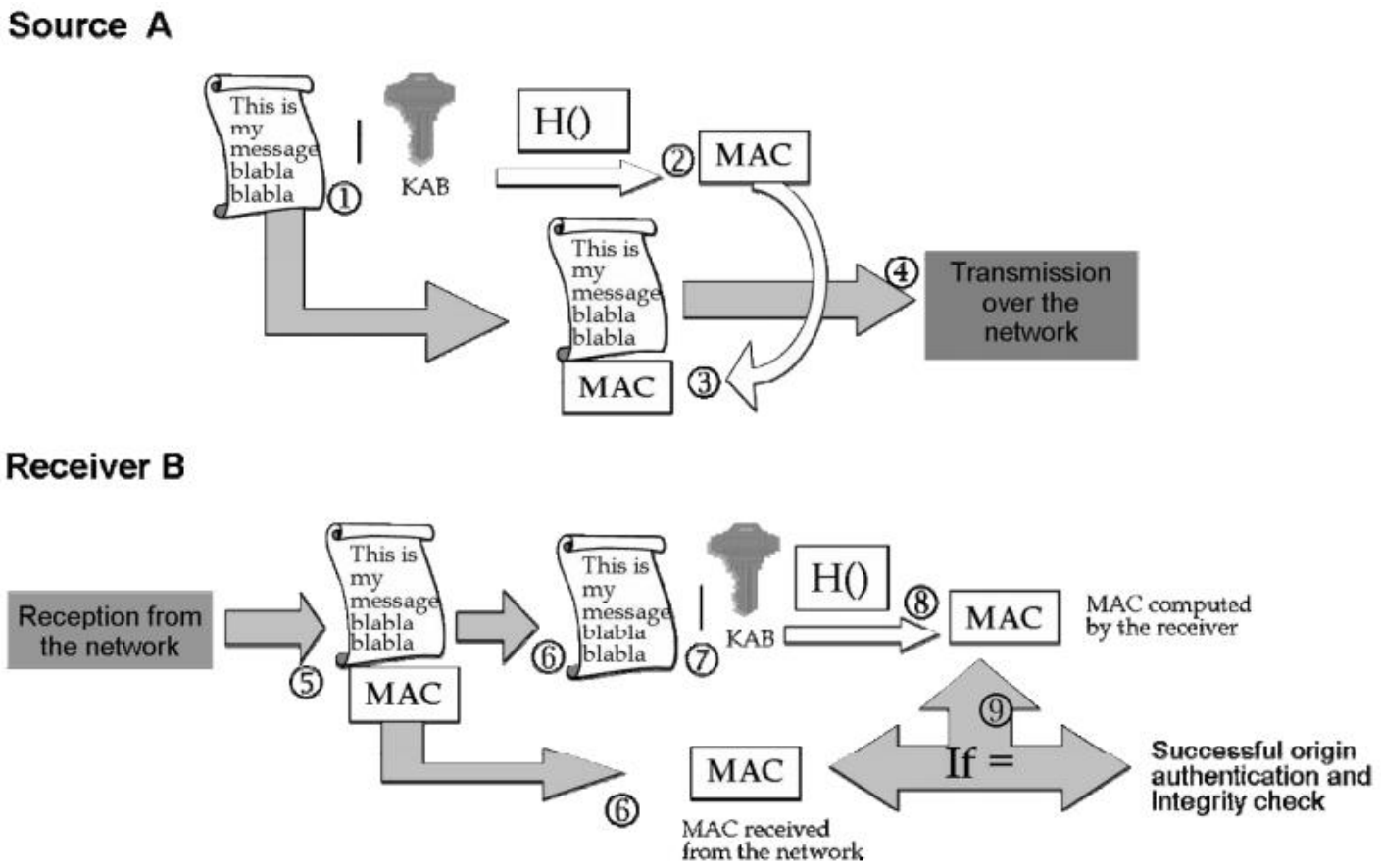


Figure 3.1. *Generation and verification of a MAC (symmetric cryptography)*

Chữ ký điện tử

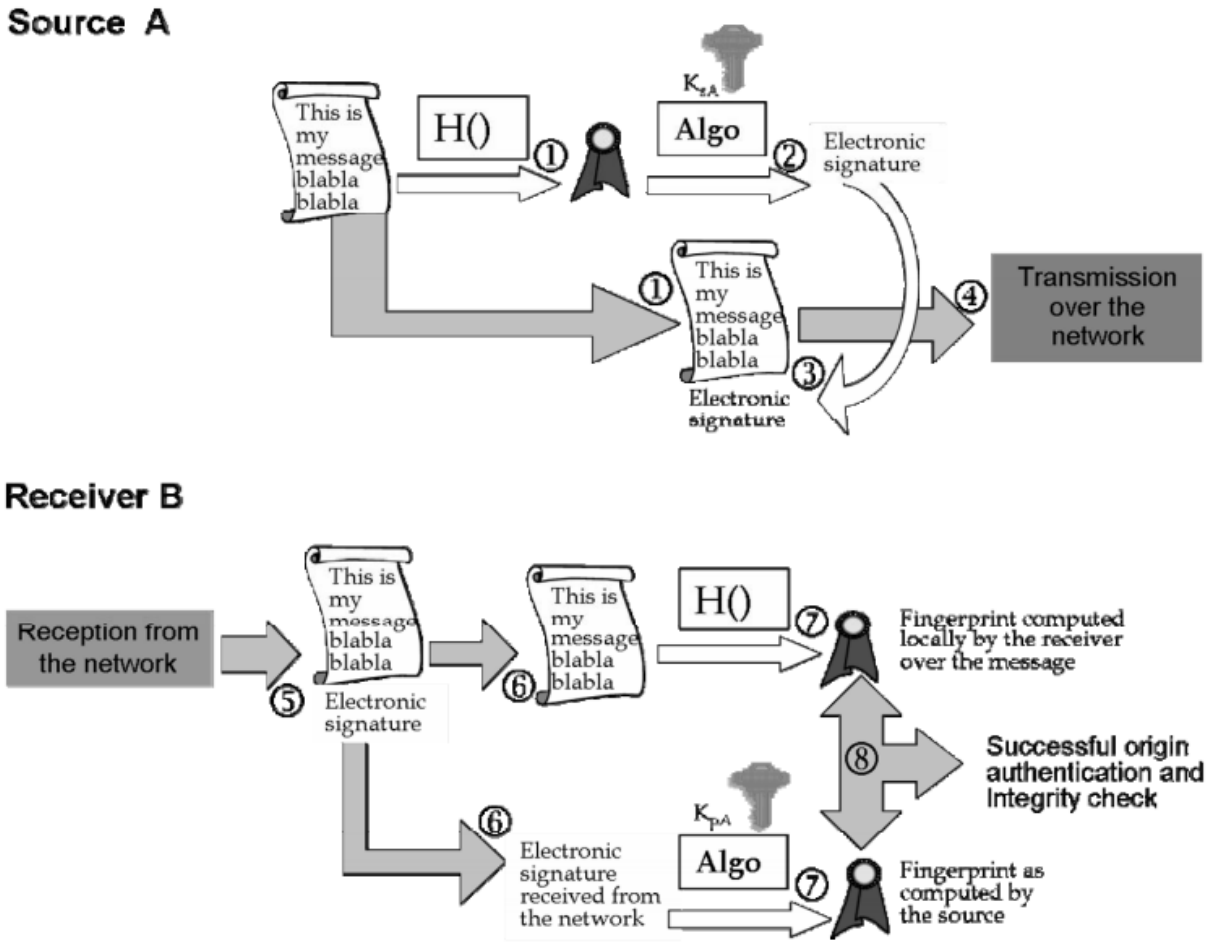


Figure 3.2. *Generation and verification of an electronic signature (asymmetric cryptography)*